SMART CARD MATING PROTOCOL

BACKGROUND OF THE INVENTION

The present invention generally relates to communication systems, and more specifically to a protocol for mating a signal receiver to a device that enables access to such content as in MPEG-2 streams.

Typically, delivery of MPEG-2 streams functions as follows: first, customer set-top boxes STBs which receive the MPEG-2 stream are assigned unique identities and are authorized for particular services or content through the use of individual Entitlement Management Messages (EMMs). EMMs are control messages that convey access privileges to subscriber terminals. Unlike ECMs (Entitlement Control Messages)(discussed below) which are embedded in transport multiplexes and are broadcast to multiple subscribers, EMMs are sent unicast-addressed to each subscriber terminal. That is, an EMM is specific to a particular subscriber. In a typical implementation, an EMM contains information about a key, as well as information that allows a subscriber terminal to access an ECM which is sent later. EMMs also define the tiers for each subscriber. With reference to cable services, for example, a first EMM may allow access to HBO™, ESPN™ and CNN™. A second EMM may allow access to ESPN™, TNN™ and BET™, etc. The EMMs are generally protected such that tampering is not possible, as they enable services for which the customer has paid the provider.

Digital content is often encrypted using a series of keys, or Control Words (CWs). The content is then delivered to STBs over the transport stream, along with Entitlement Control Messages (ECMs), delivering the CWs in a protected (encrypted) fashion. In a conditional access system, each content stream is associated with a stream of ECMs that serve two basic functions: (1) to specify the access requirements for the associated content stream (i.e., what privileges are required for access to particular programs); and (2) to convey the information needed by subscriber terminals to compute the cryptographic key(s) which are needed for content decryption. ECMs are typically transmitted in-band alongside their associated content streams. Typically, ECMs are cryptographically protected by a key which changes periodically. The key is typically distributed by EMMs prior to the ECMs, as noted above.

Upon receiving an MPEG-2 stream, the STB then validates that the STB is authorized by its EMM to access the delivered content; if authorization is validated, the ECMs are used to extract the CWs and decrypt the content. If not authorized, the STBs not allowed access to the content.

When smartcards are incorporated into such an arrangement, the unique identity is typically assigned to the smartcard, rather than the STB. The STB may also have its own identity, but this is not necessarily related to conditional access. The operation of this smartcard-inclusive conditional access arrangement is basically the same as described above, except that the STB asks the smartcard to handle EMMs, ECMs, and extraction of the CWs. The smartcard extracts the CWs and returns them to the STB for use in decrypting the content. The STB itself extracts the EMMs, ECMs, and other appropriate messages for the smartcard as well as perform the actual decryption using the CWs returned by the smartcard. The smartcard interface typically is not fast enough to perform the actual decryption of content; hence, the STB performs this task.

For best security, a smartcard, such as the MediaCipher™ smartcard produced by Motorola, Inc., is mated to its host STB in a secure fashion, such that the authorized (mated) smartcard will operate properly only when inserted into the authorized host STB. Exchanges of information between the host STB and the smartcard are protected (encrypted and/or authenticated), to guard against extraction and piracy of the exchanged information. Additionally, mating helps guard against the "mobile" smartcard scenario in which, for example, a customer authorizes the smartcard in his home, and then carries it to a local bar to enable authorization for public viewing of an event—generally undesirable for MSOs (multiple system operators).

In such an arrangement, the smartcard should mate uniquely to one host STB, and the smartcard should not operate when inserted into any host STB other than its mate. Further, exchanges of information between the host STB and the smartcard should be protected so that the interface is not vulnerable to non-intrusive snooping (i.e., monitoring the interface and observing the flows of information).

BRIEF SUMMARY OF THE INVENTION

A system is provided for uniquely mating components of a communication network such as a smartcard and a set-top box. When mated, the smartcard and set-top box are tied together and have a single identity. Further, all communication between both components are secured by encryption and authentication to prevent piracy of the exchanged information.

According to a first aspect of the invention, the system provides the same authentication key to the set-top box and the smartcard. This authentication key is used for authenticating all communication between the set-top box and the smartcard. Initially, the authentication key is encrypted by a set-top box mating key. The set-top box employs this mating key to decrypt the authentication key. After it is derived, the authentication key is stored in the set-top box's memory. Further, the same authentication key is encrypted by a smartcard mating key. Thereafter, the smartcard employs the smartcard mating key to extract the authentication key.

Note that the clear authentication key is stored in the smartcard's memory as well. In this manner, the authentication key is used for securing all communication between the set-top box and the smart-card. For example, the set-top box may request control words from the smartcard. Only after the request is authenticated, are the control words for decrypting digital content provided to the set-top box. If the smartcard authentication key is different from the set-top box key, the request for control words is denied. Also, the authentication key may be used for encryption.

According to another aspect of the present invention, a hashed authentication key is used for authenticating information exchanges between the smartcard and the set-top box. The hashed authentication key is computed using a protocol nonce that is provided to both the smartcard and the set-top box.

According to another aspect of the invention, a set-top provisioning key is provided. This key is used by the smartcard for encrypting the set-top mating key. Thereafter, the encrypted set-top mating key is forwarded to the set-top box. The set-top box then employs the provisioning key to extract the set-top mating key. In turn, the set-top mating key is employed for extracting the authentication key. Note that the provisioning key is symmetrical, and may be randomly generated by the set-top box. After generation, the provisioning key is securely transmitted to the smartcard. This eliminates the need for entering a key or secret code into the